ELLIPTIC CURVE CRYPTOGRAPHIC METHODS AND APPARATUS

Abstract

Methods for generating elliptic curves of known order over finite fields include selecting a discriminant and a class polynomial from respective sets of discriminants and class polynomials. Based on the selected values, an order of an elliptic curve is determined and the elliptic curve is specified based on a root of the class polynomial. The order of the elliptic curve is adjusted based on a twist operation. The methods are implemented in, for example, computer executable instructions stored on a computer readable medium. Elliptic curve generators based on the methods are provided as well as cryptographic systems including such generators.